WHAT IS CLAIMED IS:

1. A copyright protection system comprising:

an encryption device and a decryption device, wherein cryptographic communication is performed between the encryption device and the decryption device using a contents key,

wherein the encryption device includes

a contents storage section for storing contents,

a first contents key generation section for generating the contents key based on a second decryption limitation obtained by updating a first decryption limitation, and

a first encryption section for encrypting the contents using the contents key and outputting the encrypted contents, and

wherein the decryption device includes

a second contents key generation section for generating the contents key from the second decryption limitation, and

a first decryption section for decrypting the encrypted contents using the contents key generated by the second contents key generation section.

2. A copyright protection system according to claim 1,

wherein the decryption device further includes

a decryption limitation updating section for updating the first decryption limitation to the second decryption limitation in accordance with a decryption limitation updating rule, and

a second encryption section for encrypting the second decryption limitation using a time-varying key, and

outputting the first encrypted decryption limitation,

wherein the encryption device further includes a second decryption section for decrypting the first encrypted decryption limitation transferred from the second encryption section using the time-varying key to generate the second decryption limitation,

wherein the first contents key generation section generates the contents key based on the second decryption limitation generated by the second decryption section.

3. A copyright protection system according to claim 2, wherein the encryption device further includes

a first common key storage section for storing a common key,

a decryption limitation storage section for storing the first decryption limitation,

a first random number generation section for generating a first random number,

a first mutual authentication section for performing mutual authentication in association with the decryption device using the first random number, and a second random number transferred from the decryption device,

a first time-varying key generation section for generating the time-varying key using the first random number and the second random number in response to the authentication by the first mutual authentication section, and

a third encryption section for encrypting the first decryption limitation using the time-varying key and outputting the second encrypted decryption limitation, and

wherein the decryption device further includes

a second common key storage section for storing the common key,

a second random number generation section for generating the second random number,

a second mutual authentication section for performing mutual authentication in association with the encryption device using the second random number and the first random number,

a second time-varying key generation section for generating the time-varying key using the second random number and the first random number in response to the authentication by the second mutual authentication section, and

a third decryption section for decrypting the second encrypted decryption limitation using the time-varying key.

4. A copyright protection system according to claim 1, wherein the decryption device further includes a first decryption limitation updating section for updating the first decryption limitation to the second decryption limitation in accordance with a decryption limitation updating rule, and

a second contents key generation section for generating the contents key based on the second decryption limitation updated by the first decryption limitation updating section,

wherein the encryption device further includes a second decryption limitation updating section for updating the first decryption limitation to the second decryption limitation in accordance with the decryption limitation updating rule in response to the updating of the first decryption limitation by the first decryption limitation updating section,

the first contents key generation section generates

the contents key based on the second decryption limitation updated by the first decryption limitation updating section.

5. A copyright protection system according to claim 4, wherein the encryption device further includes

a first common key storage section for storing a common key,

a decryption limitation storage section for storing the first decryption limitation,

a first random number generation section for generating a first random number,

a first mutual authentication section for performing mutual authentication in association with the decryption device using the first random number, and a second random number transferred from the decryption device,

a first time-varying key generation section for generating a time-varying key using the first random number and the second random number in response to the authentication by the first mutual authentication section, and

a second encryption section for encrypting the first decryption limitation using the time-varying key and outputting an encrypted decryption limitation, and

wherein the decryption device further includes

a second common key storage section for storing the common key,

a second random number generation section for generating the second random number,

a second mutual authentication section for performing mutual authentication in association with the encryption device using the second random number and the first random number,

a second time-varying key generation section for generating the time-varying key using the second random number and the first random number in response to the authentication by the second mutual authentication section, and

a second decryption section for decrypting the encrypted decryption limitation using the time-varying key.

6. A copyright protection system according to claim 5, wherein the second decryption limitation updating section updates the first decryption limitation to the second decryption limitation in advance,

the first contents key generation section generates the contents key from the second decryption limitation, and

the second decryption limitation updating section stores the second decryption limitation in the decryption limitation storage section in response to the start of processing by the first encryption section.

7. A copyright protection system according to claim 3, wherein the first and second time-varying key generation sections generate the time-varying key based on the first and second random numbers and the common key.

8. A copyright protection system according to claim 3, wherein the first and second contents key generation sections generate the contents key based on the second decryption limitation and the time-varying key.

9. A copyright protection system according to claim 3, wherein the encryption device and the decryption device further include respective first and second data sequence key generation sections for generating a data sequence key

based on a data sequence input to or output from the encryption device and the decryption device, and

wherein the first and second time-varying key generation sections generate the time-varying key based on the first and second random numbers and the respective data sequence key.

10. A copyright protection system according to claim 3, wherein the encryption device and the decryption device further include respective first and second data sequence key generation sections for generating a data sequence key based on a data sequence input to or output from the encryption device and the decryption device, and

wherein the first and second time-varying key generation sections generate the time-varying key based on the first and second random numbers, the common key, and the respective data sequence key.

11. A copyright protection system according to claim 3, wherein the encryption device and the decryption device further include respective first and second data sequence key generation sections for generating a data sequence key based on a data sequence input to or output from the encryption device and the decryption device, and

wherein the first and second contents key generation sections generate the contents key based on the second decryption limitation and the respective data sequence key.

12. A copyright protection system according to claim 3, wherein the encryption device and the decryption device further include respective first and second data sequence key generation sections for generating a data sequence key based on a data sequence input to or output from the

encryption device and the decryption device, and

wherein the first and second contents key generation section generate the contents key based on the second decryption limitation, the time-varying key, and the respective data sequence key.

13. A copyright protection system according to claim 3, wherein the first and second mutual authentication sections mutually authenticate the decryption device and the encryption device, respectively, by communication in accordance with a challenge-response type authentication protocol.

14. An encryption device for performing cryptographic communication in association with a decryption device using a contents key, comprising:

a contents storage section for storing contents;

a contents key generation section for generating the contents key based on a second decryption limitation obtained by updating a first decryption limitation; and

a first encryption section for encrypting the contents using the contents key and outputting the encrypted contents.

15. An encryption device according to claim 14, further including a decryption section for decrypting the first encrypted decryption limitation .transferred from the decryption device using the time-varying key to generate the second decryption limitation, and

the contents key generation section generates the contents key based on the second decryption limitation generated by the decryption device.

16. An encryption device according to claim 15, further including

a common key storage section for storing a common key,

a decryption limitation storage section for storing the first decryption limitation,

a first random number generation section for generating a first random number,

a mutual authentication section for performing mutual authentication in association with the decryption device using the first random number, and a second random number transferred from the decryption device,

a time-varying key generation section for generating the time-varying key using the first random number and the second random number in response to the authentication by the mutual authentication section, and

a second encryption section for encrypting the first decryption limitation using the time-varying key and outputting the second encrypted decryption limitation.

17. An encryption device according to claim 14, further including a decryption limitation updating section for updating the first decryption limitation to the second decryption limitation in accordance with a decryption limitation updating rule in response to the updating of a decryption limitation by the decryption device,

wherein the contents key generation section generates the contents key based on the second decryption limitation obtained by the decryption limitation updating section.

18. An encryption device according to claim 17, further including

a common key storage section for storing a common key,

a decryption limitation storage section for storing the first decryption limitation,

a first random number generation section for generating a first random number,

a mutual authentication section for performing mutual authentication in association with the decryption device using the first random number, and a second random number transferred from the decryption device,

a time-varying key generation section for generating a time-varying key using the first random number and the second random number in response to the authentication by the mutual authentication section, and

a second encryption section for encrypting the first decryption limitation using the time-varying key and outputting an encrypted decryption limitation.

19. An encryption device according to claim 17, wherein:

the decryption limitation updating section updates the first decryption limitation to the second decryption limitation in advance;

the decryption limitation updating section outputs the second decryption limitation to the contents key generation section;

the contents key generation section generates the contents key from the second decryption limitation; and

the decryption limitation updating section stores the second decryption limitation in the decryption limitation storage section in response to the start of processing by the first encryption section.

20. An encryption device according to claim 16, wherein the

time-varying key generation section generates the time-varying key based on the first and second random numbers and the common key.

21. An encryption device according to claim 16, wherein the contents key generation section generates the contents key based on the second decryption limitation and the time-varying key.

22. An encryption device according to claim 16, further including a data sequence key generation section for generating a data sequence key based on a data sequence input to or output from the encryption device,

the time-varying key generation section generates the time-varying key based on the first and second random numbers and the data sequence key.

23. An encryption device according to claim 16, further including a data sequence key generation section for generating a data sequence key based on a data sequence input to or output from the encryption device,

wherein the time-varying key generation section generates the time-varying key based on the first and second random numbers, the common key, and the data sequence key.

24. An encryption device according to claim 16, further including a data sequence key generation section for generating a data sequence key based on a data sequence input to or output from the encryption device,

wherein the contents key generation section generates the contents key based on the second decryption limitation and the data sequence key.

25. An encryption device according to claim 16, further including a data sequence key generation section for generating a data sequence key based on a data sequence input to or output from the encryption device,

wherein the contents key generation section generates the contents key based on the second decryption limitation, the time-varying key, and the data sequence key.

26. A decryption device for performing cryptographic communication in association with an encryption device using a contents key, comprising:

a contents key generation section for generating the contents key from a second decryption limitation; and

a first decryption section for decrypting encrypted contents using the contents key generated by the contents key generation section.

27. A decryption device according to claim 26, further including

a decryption limitation updating section for updating a first decryption limitation to the second decryption limitation in accordance with a decryption limitation updating rule, and

an encryption section for encrypting the second decryption limitation using a time-varying key, and outputting the first encrypted decryption limitation.

28. A decryption device according to claim 27, further including

a common key storage section for storing the common key,

a random number generation section for generating the second random number,

a mutual authentication section for performing mutual authentication in association with the encryption device using the second random number and a first random number,

a time-varying key generation section for generating the time-varying key using the second random number and the first random number in response to the authentication by the mutual authentication section, and

a second decryption section for decrypting a first encrypted decryption limitation using the time-varying key.

29. A decryption device according to claim 26, further including a decryption limitation updating section for updating the first decryption limitation to a second decryption limitation in accordance with a decryption limitation updating rule,

wherein a contents key generation section for generating the contents key based on the second decryption limitation updated by the decryption limitation updating section.

30. A decryption device according to claim 29, further including

a second common key storage section for storing the common key,

a second random number generation section for generating the second random number,

a mutual authentication section for performing mutual authentication in association with the encryption device using the second random number and a first random number,

a time-varying key generation section for generating the time-varying key using the second random

number and the first random number in response to the authentication by the mutual authentication section, and

a second decryption section for decrypting encrypted decryption limitation using the time-varying key.

31. A decryption device according to claim 28, wherein the time-varying key generation section generates the time-varying key based on the first and second random numbers and the common key.

32. A decryption device according to claim 28, wherein the contents key generation section generates the contents key based on the second decryption limitation and the time-varying key.

33. A decryption device according to claim 28, further including a data sequence key generation section for generating a data sequence key based on a data sequence input to or output from the decryption device,

wherein the time-varying key generation section generates the time-varying key based on the first and second random numbers and the data sequence key.

34. A decryption device according to claim 28, further including a data sequence key generation section for generating a data sequence key based on a data sequence input to or output from the decryption device,

wherein the time-varying key generation section generates the time-varying key based on the first and second random numbers, the common key, and the data sequence key.

35. A decryption device according to claim 28, further including a data sequence key generation section for

generating a data sequence key based on a data sequence input to or output from the decryption device,

wherein the contents key generation section generates the contents key based on the second decryption limitation and the data sequence key.

36. A decryption device according to claim 28, further including a data sequence key generation section for generating a data sequence key based on a data sequence input to or output from the decryption device,

wherein the contents key generation section generates the contents key based on the second decryption limitation, the time-varying key, and the data sequence key.

37. A recording medium storing a program for use in causing a computer to perform cryptographic communication with an encryption device using a contents key, wherein:

the program causes the computer to function as:

a contents key generation section for generating the contents key from a second decryption limitation; and

a first decryption section for decrypting encrypted contents using the contents key generated by the contents key generation section.

38. A recording medium according to claim 37, wherein the program causes the computer to further function as:

a decryption limitation updating section for updating a first decryption limitation to the second decryption limitation in accordance with a decryption limitation updating rule; and

an encryption section for encrypting the second decryption limitation using a time-varying key, and

outputting a first encrypted decryption limitation.

39. A recording medium according to claim 38, wherein the program causes the computer to further function as:

a common key storage section for storing the common key;

a random number generation section for generating a second random number;

a mutual authentication section for performing mutual authentication in association with the encryption device using the second random number and a first random number;

a time-varying key generation section for generating the time-varying key using the second random number and the first random number in response to the authentication by the mutual authentication section; and

a second decryption section for decrypting a first encrypted decryption limitation using the time-varying key.

40. A recording medium according to claim 37, wherein:

the program causes the computer to further function as a decryption limitation updating section for updating a first decryption limitation to the second decryption limitation in accordance with a decryption limitation updating rule; and

a contents key generation section for generating the contents key based on the second decryption limitation obtained by the decryption limitation updating section.

41. A recording medium according to claim 40, wherein the program causes the computer to further function as:

a second common key storage section for storing the common key;

a second random number generation section for generating the second random number;

a mutual authentication section for performing mutual authentication in association with the encryption device using the second random number and a first random number;

a time-varying key generation section for generating a time-varying key using the second random number and the first random number in response to the authentication by the mutual authentication section; and

a second decryption section for decrypting encrypted decryption limitation using the time-varying key.

42. A recording medium according to claim 39, wherein the time-varying key generation section generates the time-varying key based on the first and second random numbers and the common key.

43. A recording medium according to claim 39, wherein the contents key generation section generates the contents key based on the second decryption limitation and the time-varying key.

44. A recording medium according to claim 39, wherein:

the program causes the computer to further function as a data sequence key generation section for generating a data sequence key based on a data sequence input to or output from a decryption device; and

the time-varying key generation section generates the time-varying key based on the first and second random numbers and the data sequence key.

45. A recording medium according to claim 39, wherein:

the program causes the computer to further function as a sequence key generation section for generating a data sequence key based on a data sequence input to or output from a decryption device; and

the time-varying key generation section generates the time-varying key based on the first and second random numbers, the common key, and the data sequence key.

46. A recording medium according to claim 39, wherein:

the program causes the computer to further function as a data sequence key generation section for generating a data sequence key based on a data sequence input to or output from a decryption device; and

the contents key generation section generates the contents key based on the second decryption limitation and the data sequence key.

47. A recording medium according to claim 39, wherein:

the program causes the computer to further function as a data sequence key generation section for generating a data sequence key based on a data sequence input to or output from a decryption device; and

the contents key generation section generates the contents key based on the second decryption limitation, the time-varying key, and the data sequence key.